County of Los Angeles
CHIEF EXECUTIVE OFFICE
713 KENNETH HAHN HALL OF ADMINISTRATION
LOS ANGELES, CALIFORNIA 90012
(213) 974-1101

WILLIAM T FUJIOKA
Chief Executive Officer

March 20, 2008

To: Supervisor Yvonne B. Burke, Chair
Supervisor Gloria Molina
Supervisor Zev Yaroslavsky
Supervisor Don Knabe
Supervisor Michael D. Antonovich

From: William T Fujioka
Chief Executive Officer

CONTRACTOR ACCESS TO SENSITIVE AND CONFIDENTIAL INFORMATION

On October 23, 2007 on a motion by Supervisor Burke, the Board directed the Chief Executive Office (CEO) in conjunction with the Chief Information Office (CIO) and County Counsel to examine policies related to vendors and implement measures to improve security for confidential and sensitive information that they may be able to access. It further required that a comprehensive inventory and risk assessment be conducted to determine the extent of access by vendors to sensitive and confidential information that is maintained by the County and report back to the Board within 60 days.

On December 20, 2007, the Board granted our office an extension to March 21, 2008, to be able to collect and analyze requested vendor access information from departments and recommend new policies for your Board's consideration. This report is in keeping with the stated intent.

1. **The number of contractors utilizing "County-owned" computers as part of their contractual obligations and/or routine course of business.**

Based on the responses received from most departments to a contract inventory request submitted by CIO to all County departments, there are 1,672 contractors in this category. Some of the contractors have incidental access to sensitive/confidential information in the performance of their contracts. Most of the contractors are associated with the Department of Community and Senior Services, Department of Mental Health, Department of Public Social Services and Department of Public Works.

2. **The number of contractors with the capability of accessing or downloading employee and/or client confidential information from County data systems.**

Based on the department responses to the CIO's contract inventory request referred to in item 1 above, there are 1,737 contractors in this category. Most of the contractors are associated with the Department of Community and Senior Services, Department of Mental Health, Department of Public Health and Department of Public Social Services.

3. **The number of contractors whose own computers contain confidential information pertinent to County employees and/or clients.**

Based on the department responses to the CIO's contract inventory request referred to in item 1 above, there are 2,872 contractors in this category with the majority having access to County client information in support of programmatic services. Most of the contractors (1,472) are associated with the Department of Children and Family Services. However, there are additional contractors in this category associated with the Department of Mental Health, Department of Public Health and Department of Public Social Services. Where a contractor has access to employee information, this information is not generally maintained on contractor computers.

4. **The number of contractors who have access to portable storage devices (e.g. mobile hard drives, flash drives, etc.) containing any confidential information relevant to County employees or recipients of County services.**

It can be assumed that all contractors in items 1, 2, and 3 above have access to portable storage devices. The number of contractors in this category is impossible to determine since portable storage devices are very easy and inexpensive to acquire and use. However, the downloading of sensitive or confidential information to these devices must be in compliance with County policies and approved by departmental management.

Board Policy 6.110 - Protection of Information on Portable Computing Devices addresses the placement (downloading or inputting) of personal or confidential information on portable computing devices (e.g., laptops, tablet computers, personal digital assistants, DVDs and USB drives). This policy provides that a department manager must approve and sign the policy's attached form, entitled "Authorization to Place Personal and/or Confidential Information on a Portable Computing Device," prior to the placement of specified personal or confidential information on a specified portable computing device. The policy also requires that the recipient (person using the portable computing device) must also sign the Authorization indicating acceptance of the information and acknowledging his/her understanding of his/her responsibility to protect the information.

The Authorization sets forth certain required steps for each initial placement of personal or confidential information on a portable computing device. These steps include: (1) the portable computing device must be described in the Authorization, (2) the information to be placed on the device must be specified in the Authorization, (3) the information must be encrypted during the entire time that it resides on the device, (4) an exact copy of the information must be made (preferably on a department computer), and (5) physical security over the device must be maintained at all times (e.g., the user must maintain physical possession of the device or keep the device secure when unattended). The policy requires that each Authorization must be reviewed and renewed, at a minimum, annually.

5. Determine in which instances confidential employee and/or client information is necessary to be accessible by or given to contractors.

Where contractor access to confidential employee and/or client information is allowed, there should be a contract in place that requires the contractor to perform its work in accordance with contract provisions, including confidentiality requirements. Contractor access to such information should be determined on a contract-by-contract basis and depends upon the contractor's need for the information.

Board Policy 6.101 - Use of County Information Technology Resources provides that all persons, whether County employees, contractors, or other persons, who use County information technology assets (e.g., computers, networks, systems and data on County systems) must sign the policy's attached form, entitled "Agreement for Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data," prior to being granted access to such assets and that the Agreement must also be approved and signed by a department manager. The Agreement includes provisions addressing the access to and disclosure of County data and information.

Also, as discussed in item 4 above, Board Policy 6.110 - Protection of Information on Portable Computing Devices, provides that a department manager must approve and sign the policy's attached form, entitled "Authorization to Place Personal and/or Confidential information on a Portable Computing Device," prior to the placement of personal or confidential information on a portable computing device. Additionally, the person using the device must also sign the Authorization prior to the placement of personal or confidential information on the device.

6. Determine the feasibility of encrypting confidential information as a regular course of business and only making it accessible upon the department head's written authorization.

Board Policy 6.110 - Protection of Information on Portable Computing Devices requires all County-owned or provided portable computing devices (e.g., laptops, tablet computers, personal digital assistants, DVDs and USB drives) to be completely encrypted at all times. The policy also requires personal and confidential information to be encrypted while on any portable computing device. As discussed in items 4 and 5 above, the policy further requires prior written approval by department management to place personal or confidential information on any portable computing device, whether for use by a County employee or contractor. Given that the policy in place requires department management approval for the placement of personal or confidential information on a portable computing device, we do not recommend the additional requirement for department head approval.

Personal and confidential information is not encrypted as a matter of course on non-portable computing devices (e.g., servers and desktops). However, physical security and system access controls are in place to prevent actual or deliberate exposure of information.

7. Determine how current and recommended security policies can be included in all future contracts.

The Internal Services Department (ISD) is working with County Counsel to revise certain provisions of the Sample Contract of ISD's Model Request for Proposals relating to confidentiality and compliance with applicable law. These provisions currently require a contractor to comply will all applicable federal, state and local laws, rules, regulations, ordinances and directives. The revised provisions will additionally require that a contractor must comply with all applicable federal, state and local policies, procedures and guidelines, which would include, for example, County policies regarding information technology security and the protection of confidential records and information.

We have examined existing contractor access to sensitive and confidential information and will continue to maintain control over that access. Existing policies will be enforced and additional improvements will be added regarding sensitive and confidential information where needed.

Please contact Ellen Sandt at (213) 974-1186 if you have any questions or need additional information, or your staff may contact James Yun at (213) 893-2072.

C: Executive Officer, Board of Supervisors
County Counsel
Chief Information Officer
Internal Services Department